or make witnesses reluctant to cooperate; and lead to suppression, alteration, or destruction of evidence.

(ii) From subsections (d)(1) through (d)(4), and (f) because providing access to records of a civil or administrative investigation and the right to contest the contents of those records and force changes to be made to the information contained therein would seriously interfere with and thwart the orderly and unbiased conduct of the investigation and impede case preparation. Providing access rights normally afforded under the Privacy Act would provide the subject with valuable information that would allow interference with or compromise of witnesses or render witnesses reluctant to cooperate; lead to suppression, alteration, or destruction of evidence; enable individuals to conceal their wrongdoing or mislead the course of the investigation; and result in the secreting of or other disposition of assets that would make them difficult or impossible to reach in order to satisfy any Government claim growing out of the investigation or proceeding.

(iii) From subsection (e)(1) because it is not always possible to detect the relevance or necessity of each piece of information in the early stages of an investigation. In some cases, it is only after the information is evaluated in light of other evidence that its relevance and necessity will be clear.

(iv) From subsections (e)(4)(G) and (H) because this system of records is compiled for law enforcement purposes and is exempt from the access provisions of subsections (d) and (f).

(v) From subsection (e)(4)(I) because to the extent that this provision is construed to require more detailed disclosure than the broad, generic information currently published in the system notice, an exemption from this provision is necessary to protect the confidentiality of sources of information and to protect privacy and physical safety of witnesses and informants. DLA will, nevertheless, continue to publish such a notice in broad generic terms as is its current practice.

[DLAR 5400.21, 51 FR 33595, Sept. 22, 1986. Redesignated at 56 FR 57803, Nov. 14, 1991, as amended at 55 FR 32913, Aug. 13, 1990; 57 FR 40609, Sept. 4, 1992; 59 FR 9668, Mar. 1, 1994; 60 FR 3088, Jan. 13, 1995; 61 FR 2916, Jan. 30, 1996; 63 FR 25772, May 11, 1998; 65 FR 18900, Apr. 10, 2000]

PART 324—DFAS PRIVACY ACT PROGRAM

Subpart A—General Information

Sec.

Subpart B—Systems of Records

Subpart C—Individual Access to Records

AUTHORITY: Pub. L. 93–579, 88 Stat 1896 (5 U.S.C. 552a).

SOURCE: 61 FR 25561, May 22, 1996, unless otherwise noted.

Subpart A—General information

§ 324.1 Issuance and purpose.

The Defense Finance and Accounting Service fully implements the policy and procedures of the Privacy Act and the DoD 5400.11-R[1], 'Department of Defense Privacy Program' (see 32 CFR part 310). This regulation supplements the DoD Privacy Program only to establish policy for the Defense Finance and Accounting Service (DFAS) and provide DFAS unique procedures.

§ 324.2 Applicability and scope.

This regulation applies to all DFAS, Headquarters, DFAS Centers, the Financial System Organization (FSO), and other organizational components. It applies to contractor personnel who have entered a contractual agreement with DFAS. Prospective contractors will be advised of their responsibilities under the Privacy Act Program.

§ 324.3 Policy.

DFAS personnel will comply with the Privacy Act of 1974, the DoD Privacy Program and the DFAS Privacy Act

[1] Copies may be obtained at cost from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

Program. Strict adherence is required to ensure uniformity in the implementation of the DFAS Privacy Act Program and to create conditions that will foster public trust. Personal information maintained by DFAS organizational elements will be safeguarded. Information will be made available to the individual to whom it pertains to the maximum extent practicable. Specific DFAS policy is provided for Privacy Act training, responsibilities, reporting procedures and implementation requirements. DFAS Components will not define policy for the Privacy Act Program.

§ 324.4 Responsibilities.

(a) *Director, DFAS.* (1) Ensures the DFAS Privacy Act Program is implemented at all DFAS locations.

(2) The Director, DFAS, will be the Final Denial Appellate Authority. This authority may be delegated to the Director for Resource Management.

(3) Appoints the Director for External Affairs and Administrative Support, or a designated replacement, as the DFAS Headquarters Privacy Act Officer.

(b) *DFAS Headquarters General Counsel.* (1) Ensures uniformity is maintained in legal rulings and interpretation of the Privacy Act.

(2) Consults with DoD General Counsel on final denials that are inconsistent with other final decisions within DoD. Responsible to raise new legal issues of potential significance to other Government agencies.

(3) Provides advice and assistance to the DFAS Director, Center Directors, and the FSO as required, in the discharge of their responsibilities pertaining to the Privacy Act.

(4) Acts as the DFAS focal point on Privacy Act litigation with the Department of Justice.

(5) Reviews Headquarters' denials of initial requests and appeals.

(c) *DFAS Center Directors.* (1) Ensures that all DFAS Center personnel, all personnel at subordinate levels, and contractor personnel working with personal data comply with the DFAS Privacy Act Program.

(2) Serves as the DFAS Center Initial Denial Authority for requests made as a result of denying release of requested information at locations within DFAS Center authority. Initial denial authority may not be redelegated. Initial denial appeals will be forwarded to the appropriate DFAS Center marked to the attention of the DFAS Center Initial Denial Authority.

(d) *Director, FSO.* (1) Ensures that FSO and subordinate personnel and contractors working with personal data comply with the Privacy Act Program.

(2) Serves as the FSO Initial Denial Authority for requests made as a result of denying release of requested information at locations within FSO authority. FSO Initial denial authority may not be redelegated.

(3) Appoints a Privacy Act Officer for the FSO and each Financial System Activity (FSA).

(e) *DFAS Headquarters Privacy Act Officer.* (1) Establishes, issues and updates policy for the DFAS Privacy Act Program and monitors compliance. Serves as the DFAS single point of contact on all matters concerning Privacy Act policy. Resolves any conflicts resulting from implementation of the DFAS Privacy Act Program policy.

(2) Serves as the DFAS single point of contact with the Department of Defense Privacy Office. This duty may be delegated.

(3) Ensures that the collection, maintenance, use and/or dissemination of records of identifiable personal information is for a necessary and lawful purpose, that the information is current and accurate for the intended use and that adequate security safeguards are provided.

(4) Monitors system notices for agency systems of records. Ensures that new, amended, or altered notices are promptly prepared and published. Reviews all notices submitted by the DFAS Privacy Act Officers for correctness and submits same to the Department of Defense Privacy Office for publication in the FEDERAL REGISTER. Maintains and publishes a listing of DFAS Privacy Act system notices.

(5) Establishes DFAS Privacy Act reporting requirement due dates. Compiles all Agency reports and submits the completed annual report to the Defense Privacy Office. DFAS reporting

requirements are provided in appendix A to this part.

(6) Conducts annual Privacy Act Program training for DFAS Headquarters (HQ) personnel. Ensures that subordinate DFAS Center and FSO Privacy Act Officers fulfill annual training requirements.

(f) *FSO and Financial System Activities (FSAs) Legal Support*. The FSO and subordinate FSA organizational elements will be supported by the appropriate DFAS-HQ or DFAS Center General Counsel office.

(g) *DFAS Center(s) Assistant General Counsel*. (1) Ensures uniformity is maintained in legal rulings and interpretation of the Privacy Act and this regulation. Consults with the DFAS-HQ General Counsel as required.

(2) Provides advice and assistance to the DFAS Center Director and the FSA in the discharge of his/her responsibilities pertaining to the Privacy Act.

(3) Coordinates on DFAS Center and the FSA denials of initial requests.

(h) *DFAS Center Privacy Act Officer*. (1) Implements and administers the DFAS Privacy Act Program for all personnel, to include contractor personnel, within the Center, Operating Locations (OpLocs) and Defense Accounting Offices (DAOs).

(2) Ensures that the collection, maintenance, use, or dissemination of records of identifiable personal information is in a manner that assures that such action is for a necessary and lawful purpose; the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information. Advises the Program Manager that systems notices must be published in the FEDERAL REGISTER prior to collecting or maintenance of the information. Submits system notices to the DFAS-HQ Privacy Act Officer for review and subsequent submission to the Department of Defense Privacy Office.

(3) Administratively controls and processes Privacy Act requests. Ensures that the provisions of this regulation and the DoD Privacy Act Program are followed in processing requests for records. Ensures all Privacy Act requests are promptly reviewed. Coordinates the reply with other organizational elements as required.

(4) Prepares denials and partial denials for the Center Director's signature and obtain required coordination with the assistant General Counsel. Responses will include written justification citing a specific exemption or exemptions.

(5) Prepares input for the annual Privacy Act Report as required using the guidelines provided in appendix A to this part.

(6) Conducts training on the DFAS Privacy Act Program for Center personnel.

(i) *FSO Privacy Act Officer*. (1) Implements and administers the DFAS Privacy Act Program for all personnel, to include contractor personnel, within the FSO.

(2) Ensures that the collection, maintenance, use, or dissemination of records of identifiable personal information is in a manner that assures that such action is for a necessary and lawful purpose; the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information. Advises the Program Manager that systems notices must be published in the FEDERAL REGISTER prior to collecting or maintenance of the information. Submits system notices to the DFAS-HQ Privacy Act Officer for review and subsequent submission to the Department of Defense Privacy Office.

(3) Administratively controls and processes Privacy Act requests. Ensures that the provisions of this regulation and the DoD Privacy Act Program are followed in processing requests for records. Ensure all Privacy Act requests are promptly reviewed. Coordinate the reply with other organizational elements as required.

(4) Prepares denials and partial denials for signature by the Director, FSO and obtains required coordination with the assistant General Counsel. Responses will include written justification citing a specific exemption or exemptions.

(5) Prepares input for the annual Privacy Act Report (RCS: DD DA&M(A)1379) as required using the

guidelines provided in appendix A to this part.

(6) Conducts training on the DFAS Privacy Act Program for FSO personnel.

(j) *DFAS employees.* (1) Will not disclose any personal information contained in any system of records, except as authorized by this regulation.

(2) Will not maintain any official files which are retrieved by name or other personal identifier without first ensuring that a system notice has been published in the FEDERAL REGISTER.

(3) Reports any disclosures of personal information from a system of records or the maintenance of any system of records not authorized by this regulation to the appropriate Privacy Act Officer for action.

(k) *DFAS system managers (SM).* (1) Ensures adequate safeguards have been established and are enforced to prevent the misuse, unauthorized disclosure, alteration, or destruction of personal information contained in system records.

(2) Ensures that all personnel who have access to the system of records or are engaged in developing or supervising procedures for handling records are totally aware of their responsibilities to protect personal information established by the DFAS Privacy Act Program.

(3) Evaluates each new proposed system of records during the planning stage. The following factors should be considered:

(i) Relationship of data to be collected and retained to the purpose for which the system is maintained. All information must be relevant to the purpose.

(ii) The impact on the purpose or mission if categories of information are not collected. All data fields must be necessary to accomplish a lawful purpose or mission.

(iii) Whether informational needs can be met without using personal identifiers.

(iv) The disposition schedule for information.

(v) The method of disposal.

(vi) Cost of maintaining the information.

(4) Complies with the publication requirements of DoD 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310). Submits final publication requirements to the appropriate DFAS Privacy Act Officer.

(l) *DFAS program manager(s).* Reviews system alterations or amendments to evaluate for relevancy and necessity. Reviews will be conducted annually and reports prepared outlining the results and corrective actions taken to resolve problems. Reports will be forwarded to the appropriate Privacy Act Officer.

(m) *Federal government contractors.* When a DFAS organizational element contracts to accomplish an agency function and performance of the contract requires the operation of a system of records or a portion thereof, DoD 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310) and this part apply. For purposes of criminal penalties, the contractor and its employees shall be considered employees of DFAS during the performance of the contract.

(1) *Contracting involving operation of systems of records.* Consistent with Federal Acquisition Regulation (FAR)[2] and the DoD Supplement to the Federal Acquisition Regulation (DFAR)[3], Part 224.1, contracts involving the operation of a system of records or portion thereof shall specifically identify the record system, the work to be performed and shall include in the solicitations and resulting contract such terms specifically prescribed by the FAR and DFAR.

(2) *Contracting.* For contracting subject to this part, the Agency shall:

(i) Informs prospective contractors of their responsibilities under the DFAS Privacy Act Program.

(ii) Establishes an internal system for reviewing contractor performance to ensure compliance with the DFAS Privacy Act Program.

(3) *Exceptions.* This rule does not apply to contractor records that are:

(i) Established and maintained solely to assist the contractor in making internal contractor management decisions, such as records maintained by

[2] Copies may be obtained at cost from the Superintendent of Documents, P.O. Box 37195, Pittsburgh, PA 15250–7954.

[3] See footnote 2 to § 324.4(m)(1)

the contractor for use in managing the contract.

(ii) Maintained as internal contractor employee records, even when used in conjunction with providing goods or services to the agency.

(4) *Contracting procedures.* The Defense Acquisition Regulatory Council is responsible for developing the specific policies and procedures for soliciting, awarding, and administering contracts.

(5) *Disclosing records to contractors.* Disclosing records to a contractor for use in performing a DFAS contract is considered a disclosure within DFAS. The contractor is considered the agent of DFAS when receiving and maintaining the records for the agency.

Subpart B—Systems of Records

§ 324.5 General information.

(a) The provisions of DoD 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310) apply to all DFAS systems of records. DFAS Privacy Act Program Procedural Rules, DFAS Exemption Rules and System of Record Notices are the three types of documents relating to the Privacy Act Program that must be published in the FEDERAL REGISTER.

(b) A system of records used to retrieve records by a name or some other personal identifier of an individual must be under DFAS control for consideration under this regulation. DFAS will maintain only those Systems of Records that have been described through notices published in the FEDERAL REGISTER.

(1) *First amendment guarantee.* No records will be maintained that describe how individuals exercise their rights guaranteed by the First Amendment unless maintenance of the record is expressly authorized by Statute, the individual or for an authorized law enforcement purpose.

(2) *Conflicts.* In case of conflict, the provisions of DoD 5400.11-R take precedence over this supplement or any DFAS directive or procedure concerning the collection, maintenance, use or disclosure of information from individual records.

(3) *Record system notices.* Record system notices are published in the FEDERAL REGISTER as notices and are not subject to the rule making procedures. The public must be given 30 days to comment on any proposed routine uses prior to implementing the system of record.

(4) *Amendments.* Amendments to system notices are submitted in the same manner as the original notices.

§ 324.6 Procedural rules.

DFAS procedural rules (regulations having a substantial and direct impact on the public) must be published in the FEDERAL REGISTER first as a proposed rule to allow for public comment and then as a final rule. Procedural rules will be submitted through the appropriate DFAS Privacy Act Officer to the Department of Defense Privacy Office. Appendix B to this part provides the correct format. Guidance may be obtained from the DFAS-HQ and DFAS Center Records Managers on the preparation of procedural rules for publication.

§ 324.7 Exemption rules.

(a) *Submitting proposed exemption rules.* Each proposed exemption rule submitted for publication in the FEDERAL REGISTER must contain: The agency identification and name of the record system for which an exemption will be established; The subsection(s) of the Privacy Act which grants the agency authority to claim an exemption for the system; The particular subsection(s) of the Privacy Act from which the system will be exempt; and the reasons why an exemption from the particular subsection identified in the preceding subparagraph is being claimed. No exemption to all provisions of the Privacy Act for any System of records will be granted. Only the Director, DFAS may make a determination that an exemption should be established for a system of record.

(b) *Submitting exemption rules for publication.* Exemption rules must be published in the FEDERAL REGISTER first as proposed rules to allow for public comment, then as final rules. No system of records shall be exempt from any provision of the Privacy Act until the exemption rule has been published in the FEDERAL REGISTER as a final rule. The DFAS Privacy Act Officer will submit

proposed exemption rules, in proper format, to the Defense Privacy Office, for review and submission to the FEDERAL REGISTER for publication. Amendments to exemption rules are submitted in the same manner as the original exemption rules.

(c) *Exemption for classified records.* Any record in a system of records maintained by the Defense Finance and Accounting Service which falls within the provisions of 5 U.S.C. 552a(k)(1) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G)-(e)(4)(I) and (f) to the extent that a record system contains any record properly classified under Executive Order 12589 and that the record is required to be kept classified in the interest of national defense or foreign policy. This specific exemption rule, claimed by the Defense Finance and Accounting Service under authority of 5 U.S.C. 552a(k)(1), is applicable to all systems of records maintained, including those individually designated for an exemption herein as well as those not otherwise specifically designated for an exemption, which may contain isolated items of properly classified information

(1) *General exemptions.* [Reserved]

(2) *Specific exemptions.* [Reserved]

Subpart C—Individual Access to Records

§ 324.8 Right of access.

The provisions of DoD 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310) apply to all DFAS personnel about whom records are maintained in systems of records. All information that can be released consistent with applicable laws and regulations should be made available to the subject of record.

§ 324.9 Notification of record's existence.

All DFAS Privacy Act Officers shall establish procedures for notifying an individual, in response to a request, if the system of records contains a record pertaining to him/her.

§ 324.10 Individual requests for access.

Individuals shall address requests for access to records to the appropriate Privacy Act Officer by mail or in person. Requests for access should be acknowledged within 10 working days after receipt and provided access within 30 working days. Every effort will be made to provide access rapidly; however, records cannot usually be made available for review on the day of request. Requests must provide information needed to locate and identify the record, such as individual identifiers required by a particular system, to include the requester's full name and social security number.

§ 324.11 Denials.

Only a designated denial authority may deny access. The denial must be in writing.

§ 324.12 Granting individual access to records.

(a) The individual should be granted access to the original record (or exact copy) without any changes or deletions. A record that has been amended is considered the original.

(b) The DFAS component that maintains control of the records will provide an area where the records can be reviewed. The hours for review will be set by each DFAS location.

(c) The custodian will require presentation of identification prior to providing access to records. Acceptable identification forms include military or government civilian identification cards, driver's license, or other similar photo identification documents.

(d) Individuals may be accompanied by a person of their own choosing when reviewing the record; however, the custodian will not discuss the record in the presence of the third person without written authorization.

(e) On request, copies of the record will be provided at a cost of $.15 per page. Fees will not be assessed if the cost is less that $30.00. Individuals requesting copies of their official personnel records are entitled to one free copy and then a charge will be assessed for additional copies.

§ 324.13 Access to medical and psychological records.

Individual access to medical and psychological records should be provided, even if the individual is a minor, unless

it is determined that access could have an adverse effect on the mental or physical health of the individual. In this instance, the individual will be asked to provide the name of a personal physician, and the record will be provided to that physician in accordance with guidance in Department of Defense 5400.11-R, 'Department of Defense Privacy Program' (see 32 CFR part 310).

§ 324.14 Relationship between the Privacy Act and the Freedom of Information Act.

Access requests that specifically state or reasonably imply that they are made under FOIA, are processed pursuant to the DFAS Freedom of Information Act Regulation. Access requests that specifically state or reasonably imply that they are made under the PA are processed pursuant to this regulation. Access requests that cite both the FOIA and the PA are processed under the Act that provides the greater degree of access. Individual access should not be denied to records otherwise releasable under the PA or the FOIA solely because the request does not cite the appropriate statute. The requester should be informed which Act was used in granting or denying access.

APPENDIX A TO PART 324—DFAS REPORTING REQUIREMENTS

By February 1, of each calendar year, DFAS Centers and Financial Systems Organizations will provide the DFAS Headquarters Privacy Act Officer with the following information:

1. Total Number of Requests for Access:

a. Number granted in whole:

b. Number granted in part:

c. Number wholly denied:

d. Number for which no record was found:

2. Total Number of Requests to Amend Records in the System:

a. Number granted in whole:

b. Number granted in part:

c. Number wholly denied:

3. The results of reviews undertaken in response to paragraph 3a of Appendix I to OMB Circular A-130[4].

[4] Copies available from the Office of Personnel Management, 1900 E. Street, Washington, DC 20415.

APPENDIX B TO PART 324—SYSTEM OF RECORDS NOTICE

The following data captions are required for each system of records notice published in the FEDERAL REGISTER. An explanation for each caption is provided.

1. *System identifier.* The system identifier must appear in all system notices. It is limited to 21 positions, including agency code, file number, symbols, punctuation, and spaces.

2. *Security classification.* Self explanatory. (DoD does not publish this caption. However, each agency is responsible for maintaining the information.)

3. *System name.* The system name must indicate the general nature of the system of records and, if possible, the general category of individuals to whom it pertains. Acronyms should be established parenthetically following the first use of the name (e.g., 'Field Audit Office Management Information System (FMIS)'). Acronyms shall not be used unless preceded by such an explanation. The system name may not exceed 55 character positions, including punctuation and spaces.

4. *Security classification.* This category is not published in the FEDERAL REGISTER but is required to be kept by the Headquarters Privacy Act Officer.

5. *System location.* a. For a system maintained in a single location, provide the exact office name, organizational identity, routing symbol, and full mailing address. Do not use acronyms in the location address.

b. For a geographically or organizationally decentralized system, describe each level of organization or element that maintains a portion of the system of records.

c. For an automated data system with a central computer facility and input or output terminals at geographically separate locations, list each location by category.

d. If multiple locations are identified by type of organization, the system location may indicate that official mailing addresses are published as an appendix to the agency's compilation of systems of records notices in the FEDERAL REGISTER. If no address directory is used, or if the addresses in the directory are incomplete, the address of each location where a portion of the record system is maintained must appear under the 'system location' caption.

e. Classified addresses shall not be listed but the fact that they are classified shall be indicated.

f. The U.S. Postal Service two-letter state abbreviation and the nine-digit zip code shall be used for all domestic addresses.

6. *Categories of individuals covered by the system.* Use clear, non technical terms which show the specific categories of individuals to whom records in the system pertain. Broad descriptions such as 'all DFAS personnel' or 'all employees' should be avoided unless the

term actually reflects the category of individuals involved.

7. *Categories of records in the system.* Use clear, non technical terms to describe the types of records maintained in the system. The description of documents should be limited to those actually retained in the system of records. Source documents used only to collect data and then destroyed should not be described.

8. *Authority for maintenance of the system.* The system of records must be authorized by a Federal law or Executive Order of the President, and the specific provision must be cited. When citing federal laws, include the popular names (e.g., '5 U.S.C. 552a, The Privacy Act of 1974') and for Executive Orders, the official titles (e.g., 'Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons').

9. *Purpose(s).* The specific purpose(s) for which the system of records was created and maintained; that is, the uses of the records within DFAS and the rest of the Department of Defense should be listed.

10. *Routine uses of records maintained in the system, including categories of users and purposes of the uses.* All disclosures of the records outside DoD, including the recipient of the disclosed information and the uses the recipient will make of it should be listed. If possible, the specific activity or element to which the record may be disclosed (e.g., 'to the Department of Veterans Affairs, Office of Disability Benefits') should be listed. General statements such as 'to other Federal Agencies as required' or 'to any other appropriate Federal Agency' should not be used. The blanket routine uses, published at the beginning of the agency's compilation, applies to all system notices, unless the individual system notice states otherwise.

11. *Disclosure to consumer reporting agencies.* This entry is optional for certain debt collection systems of records.

12. *Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system.* This section is divided into four parts.

13. *Storage.* The method(s) used to store the information in the system (e.g., 'automated, maintained in computers and computer output products' or 'manual, maintained in paper files' or 'hybrid, maintained in paper files and in computers') should be stated. Storage does not refer to the container or facility in which the records are kept.

14. *Retrievability.* How records are retrieved from the system (e.g., 'by name,' 'by SSN,' or 'by name and SSN') should be indicated.

15. *Safeguards.* The categories of agency personnel who use the records and those responsible for protecting the records from unauthorized access should be stated. Generally the methods used to protect the records, such as safes, vaults, locked cabinets or rooms, guards, visitor registers, personnel screening, or computer 'fail-safe' systems software should be identified. Safeguards should not be described in such detail as to compromise system security.

16. *Retention and disposal.* Describe how long records are maintained. When appropriate, the length of time records are maintained by the agency in an active status, when they are transferred to a Federal Records Center, how long they are kept at the Federal Records Center, and when they are transferred to the National Archives or destroyed should be stated. If records eventually are destroyed, the method of destruction (e.g., shredding, burning, pulping, etc.) should be stated. If the agency rule is cited, the applicable disposition schedule shall also be identified.

17. *System manager(s) and address.* The title (not the name) and address of the official or officials responsible for managing the system of records should be listed. If the title of the specific official is unknown, such as with a local system, the local director or office head as the system manager should be indicated. For geographically separated or organizationally decentralized activities with which individuals may correspond directly when exercising their rights, the position or title of each category of officials responsible for the system or portion thereof should be listed. Addresses that already are listed in the agency address directory or simply refer to the directory should not be included.

18. *Notification procedures.* Notification procedures describe how an individual can determine if a record in the system pertains to him/her. If the record system has been exempted from the notification requirements of subsection (f)(1) or subsection (e)(4)(G) of the Privacy Act, it should be so stated. If the system has not been exempted, the notice must provide sufficient information to enable an individual to request notification of whether a record in the system pertains to him/her. Merely referring to a DFAS regulation is not sufficient. This section should also include the title (not the name) and address of the official (usually the Program Manager) to whom the request must be directed; any specific information the individual must provide in order for DFAS to respond to the request (e.g., name, SSN, date of birth, etc.); and any description of proof of identity for verification purposes required for personal visits by the requester.

19. *Record access procedures.* This section describes how an individual can review the record and obtain a copy of it. If the system has been exempted from access and publishing access procedures under subsections (d)(1) and (e)(4)(H), respectively, of the Privacy Act, it should be so indicated. If the system has not been exempted, describe the procedures an individual must follow in order to review the record and obtain a copy of it, including any requirements for identity

verification. If appropriate, the individual may be referred to the system manager or another DFAS official who shall provide a detailed description of the access procedures. Any addresses already listed in the address directory should not be repeated.

20. *Contesting records procedures.* This section describes how an individual may challenge the denial of access or the contents of a record that pertains to him or her. If the system of record has been exempted from allowing amendments to records or publishing amendment procedures under subsections (d)(1) and (e)(4)(H), respectively, of the Privacy Act, it should be so stated. If the system has not been exempted, this caption describes the procedures an individual must follow in order to challenge the content of a record pertaining to him/her, or explain how he/she can obtain a copy of the procedures (e.g., by contacting the Program Manager or the appropriate DFAS Privacy Act Officer).

21. *Record source categories.* If the system has been exempted from publishing record source categories under subsection (e)(4)(I) of the Privacy Act, it should be so stated. If the system has not been exempted, this caption must describe where DFAS obtained the information maintained in the system. Describing the record sources in general terms is sufficient; specific individuals, organizations, or institutions need not be identified.

22. *Exemptions claimed for the system.* If no exemption has been established for the system, indicate 'None.' If an exemption has been established, state under which provision of the Privacy Act it is established (e.g., 'Portions of this system of records may be exempt under the provisions of 5 U.S.C. 552a(k)(2).')

PART 326—NATIONAL RECONNAISSANCE OFFICE PRIVACY ACT PROGRAM

Sec.

AUTHORITY: Pub. L. 93–579, 88 Stat 1896 (5 U.S.C. 552a).

SOURCE: 65 FR 20372, Apr. 17, 2000, unless otherwise noted.

§ 326.1 Purpose.

This part implements the basic policies and procedures outlined in the Privacy Act of 1974, as amended (5 U.S.C. 552a), and 32 CFR part 310; and establishes the National Reconnaissance Office Privacy Program (NRO) by setting policies and procedures for the collection and disclosure of information maintained in records on individuals, the handling of requests for amendment or correction of such records, appeal and review of NRO decisions on these matters, and the application of exemptions.

§ 326.2 Application.

Obligations under this part apply to all employees detailed, attached, or assigned to or authorized to act as agents of the National Reconnaissance Office. The provisions of this part shall be made applicable by contract or other legally binding action to government contractors whenever a contract is let for the operation of a system of records or a portion of a system of records.

§ 326.3 Definitions.

Access. The review or copying of a record or its parts contained in a system of records by a requester.

Agency. Any executive or military department, other establishment, or entity included in the definition of agency in 5 U.S.C. 522(f).

Control. Ownership or authority of the NRO pursuant to federal statute or privilege to regulate official or public access to records.

Disclosure. The authorized transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or government agency other than the subject of the record, the subject's designated agent, or the subject's legal guardian.